Homework 6

Mark Schulist

1)

Show that $x^2 = -1 \bmod p$ has a solution if and only if $p = 1 \bmod 4$.

Proof. ($\Longrightarrow$) Assume $x^2 = -1 \bmod p$. From the Euler criterion, $(-1)^{\frac{p-1}{2}} = 1 \bmod p$. $p = 1, 3 \bmod 4$ for $\frac{p-1}{2}$ to make sense.

- If $p = 3 \bmod 4$, then $(-1)^{\frac{3+4k-1}{2}} = (-1)^{1+2k} = -1 \bmod p$ so by Euler there is no solution.
- If $p = 1 \bmod p$, then $(-1)^{\frac{1+4k-1}{2}} = (-1)^{2k} = 1$ so there is a solution.

Hence $p = 1 \bmod 4$.

($\Longleftarrow$) Assume $p = 1 \bmod 4$. Then

$$\begin{aligned} (-1)^{\frac{p-1}{2}} &= (-1)^{2k} = 1 \\ \Longrightarrow \quad a &= x^2 \bmod p \text{ for } a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \Longrightarrow \quad -1 &= x^2 \bmod p \text{ has solution} \end{aligned} \tag{1}$$

□

2)

2.a)

$$m \in \mathbb{N}, a \in (\mathbb{Z}/m\mathbb{Z})^\times \tag{2}$$

Let h be the order of $a (\bmod m)$. Show that for all $i, j \in \mathbb{Z}$, $a_i = a^j \bmod m \Longleftrightarrow i = j \bmod h$.

Proof. ($\Longrightarrow$) Assume $a^i = a^j \bmod m$. Then $a^{i-j} = 1 \bmod m$. So $h \mid i - j \Longrightarrow i = j \bmod h$.

($\Longleftarrow$) Assume $i = j \bmod h$. Then $h \mid i - j \Longrightarrow a^{i-j} = 1 \bmod m$. So $a^i = a^j \bmod m$. □

2.b)

Show $2^n = 4 \bmod 7 \Longleftrightarrow n = 2 \bmod 3$.

The order of $2 \bmod 7$ is $h = 3$.

Proof. ($\Longrightarrow$) Suppose $2^n = 2^2 \bmod 7$. Then $n = 2 \bmod 3$ by (a).

($\Longleftarrow$) Suppose $n = 2 \bmod 3$. Then $2^n = 2^2 \bmod 7$. □

2.c)

Which $n \in \mathbb{Z}$ is $2^n = 5 \bmod 7$.

The order of $2 \bmod 7$ is $h = 3$.

$2^1 = 2, 2^4 = 2$
$2^2 = 4, 2^5 = 4$
$2^3 = 1, 2^6 = 1$

This cycle repeats so there is no $n \in \mathbb{N}$ where $2^n = 5 \bmod 7$.

2.d)

$3^n = 2 \bmod 7$

The order of $3 \bmod 7$ is 6. So 3 is a primitive root.

$3^1 = 3$
$3^2 = 2, 3^8 = 2, ..., 3^{6k+2} = 2$

So $n = 6k + 2$ for any $k \in \mathbb{Z}$. Hence $n = 2 \bmod 6$

$5^n = 4 \bmod 11$. The order of 5 mod 11 is 5.

So $5^{5k+3} = 4$ as $5^3 = 4 \bmod 11$.

So $n = 5k + 3$ for any $k \in \mathbb{Z}$. Hence $n = 3 \bmod 5$.

3)

p odd prime, g primitive root mod p.

3.a)

Show that $g^{\frac{p-1}{2}} = -1 \bmod p$.

Proof.

$$\begin{aligned} g^{\frac{p-1}{2}} &= a \bmod p \\ g^{p-1} &= a^2 \bmod p \\ \implies \quad a^2 &= 1 \bmod p \\ a &= \pm 1 \bmod p \end{aligned} \tag{3}$$

If $a = 1$, i.e. $g^{\frac{p-1}{2}} = 1 \bmod p$, then the order of g is at most $\frac{p-1}{2}$. But g is primitive so the order of $g = p - 1$ ↯.

So $a = -1$. Hence $g^{\frac{p-1}{2}} = -1 \bmod p$. □

3.b)

Show $-g$ is a primitive root if and only if $p = 1 \bmod 4$.

Proof. Let r be the order of $(-g)$.

So $(-g)^r = 1 \bmod p$.

Then write $g = -(-g)$.

$$\begin{aligned} g^2 &= (-g)^2 \bmod p \\ g^{2r} &= (-g)^{2r} \bmod p \\ g^{2r} &= 1 \bmod p \end{aligned} \tag{4}$$

So $p - 1 \mid 2r$ as g is a primitive root.

Either $r = p - 1$ or $r = \frac{p-1}{2}$. From (a) we know that $g^{\frac{p-1}{2}} = -1 \bmod p$.

$$
\begin{aligned}
(-g)^{\frac{p-1}{2}} &= (-1)^{\frac{p-1}{2}} g^{\frac{p-1}{2}} \bmod p \\
(-g)^{\frac{p-1}{2}} &= (-1)^{\frac{p-1}{2}} (-1) = (-1)^{\frac{p+1}{2}} \bmod p
\end{aligned} \tag{5}
$$

For $-g$ to be primitive, $(-g)^{\frac{p-1}{2}} \neq 1 \bmod p$. So $\frac{p+1}{2}$ must be odd if and only if $-g$ is a primitive root (by Equation 5).

Hence

$$
\begin{aligned}
\frac{p+1}{2} &= 2k+1 \\
p+1 &= 4k+2 \\
p &= 1 \bmod 4
\end{aligned} \tag{6}
$$

If $p = 3 \bmod 4$, then $(-g)^{\frac{p-1}{2}} = 1 \bmod p$, and then $-g$ would not be a primitive root.

□

4)

$p \neq 3$ prime.

4.a)

Suppose $p = 1 \bmod 3$, $a \in (\mathbb{Z}/p\mathbb{Z}^\times)$. Show $x^3 = a \bmod p$ has a solution if and only if $a^{\frac{p-1}{3}} = 1 \bmod p$.

Proof. ($\Longrightarrow$) Suppose $x^3 = a \bmod p$ has a solution.

Let $a = x^3$. Then $a^{\frac{p-1}{3}} = x^{p-1} = 1 \bmod p$.

($\Longleftarrow$) Let g be a primitive root and $a^{\frac{p-1}{3}} = 1 \bmod p$.

Write $a = g^k$ for some $k = 0, 1, 2, ..., p-2$.

Then $\left(g^k\right)^{\frac{p-1}{3}} = 1 \Longrightarrow g^{\frac{k(p-1)}{3}} = 1 \bmod p$.

Since $p-1$ is the order of g, $p-1 \mid \frac{k(p-1)}{3} \Longrightarrow 3 \mid k \Longrightarrow k = 3l$ for some $l \in \mathbb{Z}$.

So $a = g^k = g^{3l} = \left(g^l\right)^3$. Hence a is a cube. □

4.b)

Show that $\frac{1}{3}$ of the elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ are cubes.

Proof. Let g be a primitive root mod p. Then $g^k = a$ is a cube if $3 \mid k$. So every third element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cube, hence $\frac{1}{3}$ of the elements are cubes. We know that we can write all elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ as g^k for some k, so we have shown that a third of the elements are cubes. □

4.c)

$(\mathbb{Z}/13\mathbb{Z})^\times$. $g = 2$ is a primitive root.

$2^{12}, 2^9, 2^6, 2^3$ are cubes mod 13. These are all of the exponents that divide 12 of a primitive root mod 13.

4.d)

$p = 2 \bmod 3$.

There are 4 cubes mod 5, 10 cubes mod 11, 16 cubes mod 17.

My conjecture is that there are $p-1$ cubes mod p if $p = 2 \bmod 3$. So every unit is a cube if $p = 2 \bmod 3$.

We want to show that if $p = 2 \bmod 3$, every unit $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ has a unique solution to $x^3 = a \bmod p$.

Proof. Let g be a primitive root mod p, and write $a = g^k$.

We can also see that (by FLT) $a = g^{k+(p-1)} \bmod p$ and $a = g^{k+2(p-1)} \bmod p$.

So by the definition of $p = 2 \bmod 3$

$$\begin{aligned} k &= k \bmod 3 \\ k + (p-1) &= k + 1 \bmod 3 \\ k + 2(p-1) &= k + 2 \bmod 3 \end{aligned} \tag{7}$$

Hence for any k, we have found that there exists an a (with the corresponding exponent) such that a is a cube. So all units are cubes mod p if $p = 2 \bmod 3$. $\square$

5)

5.a)

$a \in (\mathbb{Z}/13\mathbb{Z})^\times$, h is order of a.

Suppose $a^4 \neq 1 \bmod 13$ and $a^6 \neq 1 \bmod 13$.

$1, 2, 3, 4, 6$ are divisors of $p - 1 = 12$. Let the order of a be h. We know that $h \mid 12$.

$h \nmid 4$ and $h \nmid 6$ but $h \mid 12$. So $h = 12$, which means that a is a primitive root mod 13.

5.b)

$a \in (\mathbb{Z}/31\mathbb{Z})^\times$, h is order of a.

$1, 2, 3, 6, 10, 15$ divide $30 = p - 1$.

Let $x = 6, y = 10, z = 15$.

If $a^x \neq 1 \bmod 31$ and $a^y \neq 1 \bmod 31$ and $a^z \neq 1 \bmod 31$, then $h = 30 \Longrightarrow a$ is a primitive root.

This statement is correct because the prime factors of 30 are $2, 3, 5$, and $\frac{30}{2} = 15$, $\frac{30}{3} = 10$, $\frac{30}{5} = 6$. Hence if we check if a to the power of these three values is not equal to one, then it can not be equal to one for any of the divisors of $p - 1$.